

# Table of Contents

<b>1 Checkpoint Integration.....</b>	<b>1</b>
<b>2 Overview.....</b>	<b>2</b>
<b>3 Baseline.....</b>	<b>3</b>
<b>4 Prerequisites.....</b>	<b>4</b>
<b>5 Gaia Configuration.....</b>	<b>5</b>
5.1 Enabling RADIUS Authentication in Gaia.....	5
<b>6 Customising the Gaia Login Page.....</b>	<b>6</b>
6.1 Test the RADIUS authentication.....	6
<b>7 Swivel Configuration.....</b>	<b>16</b>
7.1 Configuring the RADIUS server.....	16
7.2 Enabling Session creation with username.....	16
7.3 Setting up Swivel Dual Channel Transports.....	16
<b>8 Testing.....</b>	<b>20</b>
<b>9 Troubleshooting.....</b>	<b>21</b>
<b>10 Additional Information.....</b>	<b>22</b>
<b>11 MobileIron Integration.....</b>	<b>23</b>
<b>12 Overview.....</b>	<b>24</b>
<b>13 Prerequisites.....</b>	<b>25</b>
<b>14 How does it work.....</b>	<b>26</b>
<b>15 SwivelSecure Configuration.....</b>	<b>27</b>
15.1 Enabling Standard Federation - Sales Force.....	27
15.2 Enabling Standard Federation - Office 365.....	35
<b>16 Related Articles.....</b>	<b>40</b>
<b>17 Additional Information.....</b>	<b>41</b>

# **1 Checkpoint Integration**

**PINsafe to Checkpoint Gaia**  
**Integration Notes**

## **2 Overview**

Swivel can provide strong and two factor authentication to the Checkpoint Gaia. This document outlines the details required to carry this out.

## **3 Baseline**

Swivel 4.x

Checkpoint Gaia appliance version R77.30.

## 4 Prerequisites

Working Checkpoint, smart console

Swivel 4.x

Note that modifications to the Connectra login page will affect ALL users (but not the administration page).

Use of the [TURing](#), Security String Index or [SMS](#) Confirmed message will require the use of a NAT.

When a Swivel appliance VIP is used, the real IP address should be used and not the VIP. For redundancy select Primary and Secondary RADIUS servers, see [VIP on PINsafe Appliances](#).

## 5 Gaia Configuration

### 5.1 Enabling RADIUS Authentication in Gaia

You need to configure Swivel as an authentication server on the Gaia appliance.

- Open Smart Dashboard and log in.
- Under Network and Resources -> Hosts, configure the Swivel server as a new host. You just need to give it a name and add the IP address.
- Under Users and Authentication -> Authentication -> RADIUS Servers, create a new RADIUS server. Select Swivel as the host, ?NEW-RADIUS? as the service, and enter the shared secret you previously set on the Swivel server. You can select RADIUS version 1 or 2, and PAP or MSChap as the protocol: Swivel will detect these protocols automatically. Note: When a Swivel appliance VIP is used, the real IP address should be used and not the VIP. For redundancy select Primary and Secondary RADIUS servers, see [VIP on PINsafe Appliances](#).

You will also need to configure authentication for the relevant users. The simplest way to handle this is to create a new user group containing all users that will be using Swivel (if you do not already have one):

- Go to Users and Authentication -> Internal Users -> User Groups.
- Then under User Templates, create a new template, or modify an existing one, containing the relevant group, and set the authentication to RADIUS, using the Swivel server.

Don't forget to save and install the policy once you have made all relevant changes.

## 6 Customising the Gaia Login Page

**NOTE:** it is assumed here that you are familiar with Unix commands, in particular with the vi editor, as you will need to edit a file.

**NOTE:** There is an example [LoginPage.php](#) available which is the Login.php file with the modifications already included. This can be used for reference but may not be 100% suitable for specific installations and different Gaia versions.

### 6.1 Test the RADIUS authentication

At this stage it should be possible to authenticate by [SMS](#), hardware [Token](#), [Mobile Phone Client](#) and [Taskbar](#) to verify that the RADIUS authentication is working for users. Browse to the SSL VPN login page, and enter Username and if being used, the password. From the Swivel Administration console select User Administration and the required user then [View Strings](#), and select an appropriate authentication string or OTC for the user. At the SSL VPN login enter the required OTC. Check the Swivel logs for a RADIUS success or rejected message. If no RADIUS message is seen, check that the Swivel RADIUS server is started and that the correct ports are being used.

10.10.110.72 - Check Point SmartDashboard R77.30 - Mobile Access

Install Policy SmartConsole +

Firewall Application & URL Filtering Data Loss Prevention IPS Threat Prevention Anti-Spam & Mail Mobile Access IPSec VPN

**Overview**

Mobile Access allows your employees to securely read email and connect to intranet sites using a mobile device or web bro...

**My Organization**

1 Security Gateway is allowing Mobile Access [Add Gateway...](#)

	IP Address	Web	Mobile	Desktop	Compliance
VLABFWL002	10.10.110.72	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	N/A

**Users and Policy**

Active Sessions on Gateway/s: All Gateways

Users

10  
9  
8  
7  
6  
5  
4  
3  
2  
1  
0

1954:00 1954:30 1955:00 1955:30 1956:00 1956:30 1957:00 1957:30

**Network Objects**

- Check Point
  - VLABFWL002
- Nodes
- Networks
  - CP\_default\_Office\_Mode\_addresser
  - Groups
- Address Ranges
- Dynamic Objects

10.10.110.72 - Check Point SmartDashboard R77.30 - Mobile Access

Install Policy SmartConsole -

Firewall Application & URL Filtering Data Loss Prevention IPS Threat Prevention Anti-Spam & Mail Mobile Access IPSec VPN

## Overview

Mobile Access allows your employees to securely read email and connect to intranet sites using a mobile device or web browser.

### My Organization

**1 Security Gateway** is allowing traffic from the following IP Address:

VLABFWL002	10.10.110.72
------------	--------------

### Users and Policy

Active Sessions on Gateway/s: All Gateways

Time	Users
19:54:00	1

Check Point Gateway - VLABFWL002

**Check Point Gateway - General Properties**

Machine

- Name: VLABFWL002
- IPv4 Address: 10.10.110.72
- IPv6 Address: [ ]
- Comment: [ ]

Secure Internal Communication

- Communication... [ ]
- Certificate [ ]

Platform

- Hardware: Open server

Software Blades

- Network Security Blades: SG [ ]

Network Security (2) Manage

- Firewall
- IPSec VPN
- Policy Server
- Mobile Access
- IPS
- Anti-Bot
- Anti-Virus
- Anti-Spam & Email Security
- Identity Awareness
- Monitoring

Network Objects

- Check Point
  - VLABFWL002
- Nodes
- Networks
  - CP\_default\_Office\_Mode\_addresses
- Groups
- Address Ranges
- Dynamic Objects

10.10.110.72 - Check Point SmartDashboard R77.30 - Mobile Access

Install Policy SmartConsole

Firewall Application & URL Filtering Data Loss Prevention IPS Threat Prevention Anti-Spam & Mail Mobile Access IPsec VPN

**Overview**

Mobile Access allows your employees to securely read email and connect to intranet sites using a mobile device or web browser.

**My Organization**

Check Point Gateway - VLABFWL002

1 Security Gateway is allowing traffic.

IP Address

VLABFWL002 10.10.110.72

**Authentication for Mobile Access**

Authentication Method

- Defined on user record (Legacy)
- Username and password
- RADIUS
- SecurID
- Personal certificate

Name:

Two-Factor Authentication:  New...

Global setting  RADIUS

Custom settings

Allow DynamicID for mobile devices

Certificate Authentication for mobile devices

- Require client certificate when connecting
- Require client certificate when authenticating

**Users and Policy**

Active Sessions on Gateway/s: All Gateways

Time	Users
19:54:30	1
19:55:00	1
19:55:30	1
19:56:00	0
19:56:30	0
19:57:30	0

Network Objects

- Check Point
  - VLABFWL002
- Nodes
- Networks
  - CP\_default\_Office\_Mode\_addresses
- Groups
- Address Ranges
- Dynamic Objects

10.10.110.72 - Check Point SmartDashboard R77.30 - Mobile Access

Install Policy SmartConsole -

Firewall Application & URL Filtering Data Loss Prevention IPS Threat Prevention Anti-Spam & Mail Mobile Access IPSec VPN

**Overview**

Mobile Access allows your employees to securely read email and connect to intranet sites using a mobile device or web bro

**My Organization**

1 Security Gateway is allowing

IP Address  
VLABFWL002 10.10.110.72

**Users and Policy**

Active Sessions on Gateway/s: All Gateways

Users

Time	Users
19:54:30	1
19:55:00	0
19:55:30	0
19:56:00	0
19:56:30	0
19:57:00	0
19:57:30	0
19:58:00	0

Check Point Gateway - VLABFWL002

**Authentication for Mobile Access**

Authentication Method

- Defined on user record (Leave empty)
- Username and password

**RADIUS Server Properties -**

General Accounting

Name: SwivelCloud

Comment:

Color: Black

Host:

Service: UDP RADIUS

Shared Secret:

Version: RADIUS V

Protocol: PAP

Priority: 1

10.10.110.72 - Check Point SmartDashboard R77.30 - Mobile Access

Install Policy SmartConsole

Firewall Application & URL Filtering Data Loss Prevention IPS Threat Prevention Anti-Spam & Mail Mobile Access IPsec VPN

**Overview**

Mobile Access allows your employees to securely read email and connect to intranet sites using a mobile device or web browser.

**My Organization**

1 Security Gateway is allowing traffic from the following IP Address:

VLABFWL002	10.10.110.72
------------	--------------

**Host Node - demo.swivelcloud.com**

**Host Node - General Properties**

- Machine
- Name: demo.swivelcloud.com
- IPv4 Address: 52.18.78.73
- IPv6 Address:
- Comment:

**Products:**  Configure Servers...

**Users and Policy**

Active Sessions on Gateway/s: All Gateways

Time	Users
19:54:30	1
19:55:00	0
19:55:30	0
19:56:00	0
19:56:30	0
19:57:00	0
19:57:30	0
19:58:00	0

**Network Objects**

- Check Point
  - VLABFWL002
- Nodes
- Networks
  - CP\_default\_Office\_Mode\_addresses
  - Groups
- Address Ranges
- Dynamic Objects

SmartConsole -

Firewall Application & URL Filtering Data Loss Prevention IPS Threat Prevention Anti-Spam & Mail Mobile Access IPsec VPN

## Overview

Mobile Access allows your employees to securely read email and connect to intranet sites using a mobile device or web browser.

### My Organization

1 Security Gateway is allowing traffic.

IP Address
VLABFWL002 10.10.110.72

### Users and Policy

Active Sessions on Gateway/s: All Gateways

Users

19:55:30 19:56:00 19:56:30 19:57:00 19:57:30 19:58:00 19:58:30

### Check Point Gateway - VLABFWL002

- General Properties
- Topology
- NAT
- HTTPS Inspection
- HTTP/HTTPS Proxy
- Platform Portal
- VPN Clients
- Mobile Access
  - Authentication
  - Office Mode
  - Portal Customization
  - Portal Settings
  - SSL Clients
  - HTTP Proxy
  - Name Resolution
  - Link Translation
  - Endpoint Compliance
  - Check Point Secure
- Logs
- Optimizations
- Hit Count
- Other

### Authentication for Mobile Access

Authentication Method

Defined on user record (Legacy)

Username and password

### RADIUS Server Properties -

General Accounting

Name: SwivelCloud

Comment:

Color: Black

Host: demo

Service: UDP NEW-PEER

Shared Secret: \*\*\*\*\*

Version: RADIUS V

Protocol: PAP

Priority: 1



#### Network Objects

- Check Point
  - VLABFWL002
- Nodes
- Networks
  - CP\_default\_Office\_Mode\_addresses
- Groups
- Address Ranges
- Dynamic Objects

10.10.110.72 - Check Point SmartDashboard R77.30 - Mobile Access

Install Policy SmartConsole

Firewall Application & URL Filtering Data-Loss Prevention IPS Threat Prevention Anti-Spam & Mail Mobile Access IPsec VPN

**Overview**  
Mobile Access allows your employees to securely read email and connect to intranet sites using a mobile device or web browser.

**My Organization**

1 Security Gateway is allowing Mobile Access Add Gateway...

	IP Address	Web	Mobile	Desktop	Compliant
VLABFWL002	10.10.110.72	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	N/A

**Install Policy**

Install Policy  
1 gateway selected

Type to search

Installation Targets Network Sec

VLABFWL002

**Users and Policy**

Active Sessions on Gateway/s: All Gateways

Users

Advanced

10  
9  
8  
7  
6  
5  
4  
3  
2  
1  
0

19:58:30 19:59:00 19:59:30 20:00:00 20:00:30 20:01:00 20:01:30

10.10.110.72 - Check Point SmartDashboard R77.30 - Mobile Access

Install Policy SmartConsole

Firewall Application & URL Filtering Data Loss Prevention IPS Threat Prevention Anti-Spam & Mail Mobile Access IPSec VPN

**Overview**

Mobile Access allows your employees to securely read email and connect to intranet sites using a mobile device or web bro

**My Organization**

1 Security Gateway is allowing Mobile Access [Add Gateway...](#)

	IP-Address	Web	Mobile	Desktop	Compliant
VLABFWL002	10.10.110.72				N/A

Installation Process - Standard

**Installation**

Installation Targets	Version	Network S
VLABFWL002	R77.30	

**Users and Policy**

Active Sessions on Gateway/s: All Gateways

Progress

Verifying...

Show Errors...

**Network Objects**

- Check Point
  - VLABFWL002
- Nodes
- Networks
  - CP\_default\_Office\_Mode\_addresses
- Groups
- Address Ranges
- Dynamic Objects

Install Policy SmartConsole

Firewall Application & URL Filtering Data Loss Prevention IPS Threat Prevention Anti-Spam & Mail Mobile Access IPsec VPN

**Authentication**

**Allowed Authentication Schemes on Gateways**

Name	Check Point Password	SecurID
VLABPWL002	Allowed	Allowed

New... Edit... Delete

**Two-Factor Authentication with DynamicID**

Challenge users to provide the DynamicID one time password sent to their email account or mobile device via SMS.

SMS Provider and Email Settings

Specify the URL of your SMS provider, your email settings, or both. (See the online help for details and examples)

SMS provider and email settings:

SMS Provider Account Credentials (not necessary for email only):

Username:   
 Password:   
 Confirm password:   
 API ID:

Advanced...

RADIUS Server Properties -

General Accounting

Name: SwivelCloud  
 Comment:  
 Color: Black  
 Host: demo.  
 Service: UDP NEW-  
 Shared Secret: \*\*\*\*\*  
 Version: RADIUS V  
 Protocol: PAP  
 Priority: 1

**Servers and OPSEC**

- ✓ Servers
  - ✓ RADIUS
    - SwivelCloud
  - > Trusted CAs
  - OPSEC Applications

# 7 Swivel Configuration

## 7.1 Configuring the RADIUS server

On the Swivel Administration console configure the RADIUS Server and NAS, see [RADIUS Configuration](#)

## 7.2 Enabling Session creation with username

To allow the [TURing](#) image, [Pinpad](#) and other single channel images, under Server/Single Channel set [Allow session request by username](#) to Yes.

## 7.3 Setting up Swivel Dual Channel Transports

See [Transport Configuration](#)

Swivel Administration Lo Seguro | https://demo.swivelcloud.com:8080/sentry/

 swivelsecure

• [Login](#)

**Swivel Administration Login** 

Username:

OTC:

Swivel Configuration    What's My IP Address? | Seguro | https://demo.swivelcloud.com:8080/sentry/config/radius/nas

# swivelsecure

- [Status](#)
- [Log Viewer](#)
- [Server](#)
- [Policy](#)
- [Logging](#)
- [Messaging](#)
- [Database](#)
- [Mode](#)
- [Repository](#)
- [RADIUS
  - \[Server\]\(#\)
  - \[NAS\]\(#\)](#)
- [Migration](#)
- [Windows GINA](#)
- [Appliance](#)
- [OATH](#)
- [Config Sync](#)
- [Reporting](#)
- [User Administration](#)
- [Save Configuration](#)
- [Upload Email Images](#)
- [Administration Guide](#)
- [Logout](#)

## RADIUS>NAS

Please enter the details for any RADIUS network access servers. A NAS

NAS:

- [Juniper](#)
- [Netscaler](#)
- [CiscoASA](#)
- [Rob](#)
- [Watchguard](#)
- [Lisbon Forti 300C](#)
- [New Entry](#) 

Swivel Configuration    What's My IP Address? | X

Seguro | https://demo.swivelcloud.com:8080/sentry/config/radius/nas

# swivelsecure

- [Status](#)
- [Log Viewer](#)
- Server
- Policy
- Logging
- Messaging
- Database
- Mode
- Repository
- RADIUS
  - [Server](#)
  - [NAS](#)
- Migration
- Windows GINA
- Appliance
- OATH
- Config Sync
- Reporting
  - [User Administration](#)
  - [Save Configuration](#)
  - [Upload Email Images](#)
  - [Administration Guide](#)
  - [Logout](#)

## RADIUS>NAS

Please enter the details for any RADIUS network access servers. A NAS is

NAS:	<input type="checkbox"/> Juniper
	<input type="checkbox"/> Netscaler
	<input type="checkbox"/> CiscoASA
	<input type="checkbox"/> Rob
	<input type="checkbox"/> Watchguard
	<input type="checkbox"/> Lisbon_Forti_300C
	<input type="checkbox"/>
Identifier:	CheckPoint Dev
Hostname/IP:	89.114.238.196
Secret:	*****
Group:	--ANY--
EAP protocol:	<input type="button" value="None"/>
Authentication Mode:	<input type="button" value=""/>
Vendor (Groups):	<input type="button" value=""/>
Change PIN warning:	<input type="button" value="No"/>
Two Stage Auth:	<input type="button" value="No"/>
Allow blank password at Stage One:	<input type="button" value="No"/>
Send Security String after Stage One:	<input type="button" value="Yes"/>
Even if User has Valid String:	<input type="button" value="Yes"/>
Check password with repository:	<input type="button" value="No"/>
Push Enabled:	<input type="button" value="No"/>
Authenticate non-user with just password:	<input type="button" value="No"/>
Username attribute for repository:	<input type="text" value=""/>
Allow alternative usernames:	<input type="button" value="No"/>
Alternative username attributes:	<input type="text"/>
OTC timeout (mins):	<input type="text" value="0"/>
Internal IP ranges:	<input type="text"/>
Send username in challenge:	<input type="button" value="No"/>

[New Entry](#)

## 8 Testing

With the changes in place, when a user accesses the Gaia portal they will see the modified login page.

The image shows a mobile login screen for Check Point Software Technologies Ltd. The top navigation bar is blue with the 'Check Point' logo and the text 'Check Point Mob'. On the left side of the main area, there is a large, faint graphic of a key. The central part of the screen has a light blue background with the text 'Please enter your credentials' at the top. Below it, there are two input fields: 'User name' containing 'user1' and 'OTC' which is empty. Underneath these fields is a purple rectangular area labeled 'TURing' in green. This area contains a grid of numbers from 0 to 9, arranged in two rows: the top row has 1, 2, 3, 4, 5, 6, 7, 8, 9, 0; the bottom row has 5, 4, 6, 7, 8, 1, 3, 0, 2, 9. To the right of the TURing grid is a dark blue 'Sign In' button. At the bottom right of the screen, there is a 'Language:' dropdown set to 'English'.

Please enter your credentials

User name

user1

OTC

TURing

1 2 3 4 5 6 7 8 9 0

5 4 6 7 8 1 3 0 2 9

Sign In

Language: English

© Copyright 2004-2015 Check Point Software Technologies Ltd. All rights reserved.

After entering their username and either tabbing away from the username field or clicking the TURing button they will be presented with a TURing image. The PINsafe log should record a session start for that user.

The user can then use their PIN to extract their one-time code and enter this to authenticate. The PINsafe log should record the RADIUS dialogue associated with this authentication.

## 9 Troubleshooting

Check the Swivel logs for Turing images and RADIUS requests.

The screenshot shows the Swivel Log Viewer interface. On the left, there is a sidebar with various navigation links including Status, Log Viewer, Server, Policy, Logging, Messaging, Database, Mode, Repository, RADIUS, Migration, Windows GINA, Appliance, OATH, Config Sync, Reporting, User Administration, Save Configuration, Upload Email Images, Administration Guide, and Logout. The main area is titled "Swivel Log Viewer" and contains a table of log entries. The table has columns for Timestamp, Level, and Log. The log entries show RADIUS DEBUG messages related to Access Requests and Rejections. For example, one entry shows a RADIUS Access-Request message from IP 89.114.238.196 with a length of 65 bytes, containing attributes like User-Name and Service-Type. Another entry shows a RADIUS Access-Reject message with a length of 65 bytes, containing attributes like User-Name and Service-Type.

Timestamp	Level	Log
20:05:26 23/03/2017	INFO	RADIUS DEBUG: <191> Access-Request(3) LEN=65 80
20:05:26 23/03/2017	INFO	RADIUS DEBUG: <191> ----- Packets Reject(3) 000: 03 BF 00 14 0D 08 61 B6 - 97 A0 0E 4
20:05:26 23/03/2017	INFO	RADIUS DEBUG: <191> Access-Request(3) LEN=65 89
20:05:26 23/03/2017	INFO	RADIUS: <191> Access-Request(1) LEN=65 89.114.2
20:05:26 23/03/2017	INFO	AGENT_ERROR_USER_NOT_IN_GROUP
20:05:26 23/03/2017	INFO	RADIUS DEBUG: <191> Access-Request(1) LEN=65 89.114.2
20:05:26 23/03/2017	INFO	AGENT_ERROR_USER_NOT_IN_GROUP
20:05:26 23/03/2017	INFO	From the IP Address 89.114.238.196 NAS ID Lisbon_ repository to continue the authentication attempt.
20:05:26 23/03/2017	INFO	RADIUS: <191> Access-Request(1) LEN=65 89.114.2
20:05:26 23/03/2017	INFO	RADIUS DEBUG: <191> Access-Request(1) LEN=65 89
20:05:26 23/03/2017	INFO	RADIUS DEBUG: <191> ----- Packets Request(1) C00: D1 EF C0 41 8D DF 40 B9 - 71 30 D-1 79 6F 72 02 12 3A 49 3D - 58 69 A8 AC 3F A4 23 57 Attributes: User-Name (1), Length: 15, Data: [admin 0x3A493D586BABA0C]PA423571606E5564 Service-Type 0xDADA6E48 <191>
20:05:26 23/03/2017	INFO	RADIUS DEBUG: <191> Access-Request(1) LEN=65 89
20:05:21 23/03/2017	INFO	RADIUS DEBUG: <191> Access-Reject(3) LEN=65 89
20:05:21 23/03/2017	INFO	RADIUS DEBUG: <191> ----- Packets Reject(3) 000: 03 BF 00 14 0D 08 61 B6 - 97 A0 0E 4
20:05:21 23/03/2017	INFO	RADIUS DEBUG: <191> Access-Reject(3) LEN=65 89

## **10 Additional Information**

For assistance in the Swivel Secure installation and configuration please firstly contact your reseller and then email Swivel Secure support at supportdesk@swivelsecure.com

## 11 MobileIron Integration

**AuthControl Sentry/Cloud to MobileIron**

Integration Notes

## 12 Overview

Swivel Secure can provide strong and two factor authentication to the Mobile Iron. AuthControl Sentry is a linux based IdP for SAML federations. It is provided as on-prem or Cloud SaaS flavours, providing an adaptative authentication multifactor, managed by a system of points, depending on the factor used and the target app to access. This document outlines the details required to carry this out.

## **13 Prerequisites**

Working MobileIron (MobileIron Sentry appliance) MobileIron Core 9.X and Connector 9.X AuthControl Sentry 4.x

## **14 How does it work**

At App level we use conditional access to Cloud SaaS federated with SAMLv2. The Federated Identity works in 3-way trust with Access between Identity Provider (IDP), Service Provider (SP) and the Access provided by MobileIron AdminPortal/Access Gateway.

## 15 SwivelSecure Configuration

### 15.1 Enabling Standard Federation - Sales Force

The standard federation involves just this 3 fields:

- Portal URL: (this Endpoint URL can be found on the Setup -> Security Controls -> Single Sign-On

Settings page in Salesforce.com, listed as ?Salesforce Login URL? under the Endpoints section. It is unique to your Salesforce.com instance and domain.

- Entity ID:, Reflected on SalesForce SSO configuration for My Domain
- Federeated id: That needs to match with the attributed defined on Salesforce.com and Swivel

[Applications](#)[Authentication Methods](#)[View IdP Metadata](#)[Keys](#)[Users Active Sessions](#)[User History](#)[Log Viewer](#)[General Configuration](#)[Application Images](#)

## SAML Application



Note: The Endpoint URL is used only if the ACS (Assertion SAML (Security Assertion Markup Language) request.

Name

Salesforce

Image

Salesforce.png

Points

0

Portal URL

https://yourdomain.salesforce.com?

Endpoint URL

Entity ID

https://saml.sentry.salesforce.com

Federated Id

email

Once that we have a working federation from AuthControl Sentry and the SP, (in the example we will use SalesForce), this is just a standard SalesForce and Custom IdP federation on MI Access console, as the MFA part from Swivel will be triggered once the MI Access has approved the connection. AuthControl Sentry provides a metadata url to quickly get the XML from IdP. It uses POST method for federation.



Rules

Applications

Authentication Methods

View IdP Metadata

Keys

Users Active Sessions

User History

Log Viewer

General Configuration

Application Images



Swivel + SalesForce

Demo

No description

**Policy Name:** Default Policy

SAML Customization of Mobile Iron settings, Portal URL, Entity ID and Federated ID:

Name

SalesForce secured by MI Access

Image

Salesforce secured.png



Points

100

Portal URL

<https://milabses-dev-ed.my.salesforce.com?so=00D0Y0000001ktKL>

Endpoint URL

Entity ID

<https://access.mi-labs.es/MobileIron/acc/9b6d9547-11f8-4a8f-b943>

Federated Id

email

SAML Customization in the Sales Force Side. Settings for Mobile Iron.

# SAML Single Sign-On Settings

[Back to Single Sign-On Settings](#)

[Edit](#) [Delete](#) [Clone](#) [Download Metadata](#) [SAML](#)

Name	SwivelAccess
SAML Version	2.0
Issuer	<a href="https://access.mi-labs.es/MobileIron/acc/9b6d9547-11f8-4a8f-b943-e816bcc2905/idp">https://access.mi-labs.es/MobileIron/acc/9b6d9547-11f8-4a8f-b943-e816bcc2905/idp</a>
Identity Provider Certificate	C=US, ST=California, L=Mountain View, O=MobileIron, OU=Support, CN=Signing Expiration: 12 Jul 2047 08:45:42 GMT
Request Signing Certificate	<a href="#">SelfSignedCert_12Jun2017_174925</a>
Request Signature Method	RSA-SHA256
Assertion Decryption Certificate	Assertion not encrypted
SAML Identity Type	Username
SAML Identity Location	Subject
Service Provider Initiated Request Binding	HTTP POST
Identity Provider Login URL	<a href="https://access.mi-labs.es/MobileIron/acc/9b6d9547-11f8-4a8f-b943-e816bcc2905">https://access.mi-labs.es/MobileIron/acc/9b6d9547-11f8-4a8f-b943-e816bcc2905</a>
Identity Provider Logout URL	<a href="https://ssauth.mi-labs.es:8443/sentry/singlelogout">https://ssauth.mi-labs.es:8443/sentry/singlelogout</a>
Custom Error URL	

## Just-in-time User Provisioning

User Provisioning Enabled

## Endpoints

Salesforce Login URL	<a href="https://milabses-dev-ed.my.salesforce.com?so=00D0Y000001ktKL">https://milabses-dev-ed.my.salesforce.com?so=00D0Y000001ktKL</a>
OAuth 2.0 Token Endpoint	<a href="https://milabses-dev-ed.my.salesforce.com/services/oauth2/token?so=00D0Y000001ktKL">https://milabses-dev-ed.my.salesforce.com/services/oauth2/token?so=00D0Y000001ktKL</a>

[Edit](#) [Delete](#) [Clone](#) [Download Metadata](#) [SAML](#)

After the application settings definitions have been applied the applications are available in AuthControl Sentry's web portal.



Ple



SalesForce secured by MI Access

User Login in Authcontrol Sentry with SalesForce using the MI Account



sales.user@mi-labs.es

Submit

Reset

SSO for SalesForce using Mobile Iron and Turing image from SwivelSecure. This means that the user logs in using the Swivel Secure credentials, by the selected method (in this case Turing image) into the Sales Force (without the need of using Sales Force Credentials).



sales.user@mi-labs.es

Password

OTC



1	2	3	4	5	6	7	8	9	0
0	3	1	9	8	4	2	7	5	6

LoginRefresh Image

Successfull login in Sales Force.



Search...

Search

Home Chatter Campaigns Leads Accounts Contacts Opportunities



# Take Salesforce with you where

Run your business from any mobile device with the

Quick Find / Search...



[Expand All](#) | [Collapse All](#)



**Lightning Experience  
Migration Assistant**

Switch to the modern, intelligent  
Salesforce.

[Get Started](#)

## Getting Started



### Build App

Generate a basic app with just clicks or code.

[Add App](#)

## Recent Items beta

Name

## 15.2 Enabling Standard Federation - Office 365

In the case of Office365, AuthControl requires that the main federation must be performed with ADFS. On a working federation, a complement has to be installed on ADFS 3.0 server.

## Swivel Authentication Provider Configuration

Settings Languages Logging Advanced

Swivel URL: https :// ssauth.mi-labs.es : 8443 / proxy

Allow self-signed certificates

Agent Secret: XXXXXXXXXXXX

Confirm Secret: XXXXXXXXXXXX

Allow non-PINsafe users

Ignore domain prefix

Show PIN pad

Image Type: Turing

Auto-show Image

None

Turing

Image Source: Pinpad

Turing URL: https://ssauth.mi-labs.es:8443/proxy/SCImage

Pinpad URL: https://ssauth.mi-labs.es:8443/proxy/SCPinPad

OK

Cancel

Save

Swivel ADFS Authentication Provider, version 1.0.6.2, Copyright © Swivel Secure Ltd 2015

There's a couple of choices depending if the customer is using ADFS Proxy servers or not.

This plugin installs Swivel Secure product as an MFA to be applied via ADFS Authentication Policy Settings.

Set AuthControl Sentry / Swivel Secure as Authentication Provider

## Edit Global Authentication Policy

X

Primary Multi-factor

Configure multi-factor authentication (MFA) settings.

### Users/Groups

MFA is required for the following users and groups:

ES\Swivel-User-Group

Add...

Remove

### Devices

MFA is required for the following devices:

- Unregistered devices
- Registered devices

### Locations

MFA is required when accessing applications from the following locations:

- Extranet
- Intranet

Select additional authentication methods. You must select at least one of the following methods to enable MFA:

- Certificate Authentication
- Swivel Authentication Provider



[What is multi-factor authentication?](#)

OK

Cancel

Apply

On AuthControl Sentry side, we will create an Application configuration with MI Access, IdP and Office365 endpoints:



Note: The Endpoint URL is used only if the ACS (Assertion Consumer Service) is not supplied in the SAML (Security Assertion Markup Language) request.

Name

Office365 secured by MI Access

Image

O365.png



Points

100

Portal URL

<https://login.microsoftonline.com/login.srf>

Endpoint URL

<https://access.mi-labs.es/MobileIron/acc/9b7ea0b6-e908-4111-8eb1-94c>

Entity ID

<https://access.mi-labs.es/MobileIron/acc/9b7ea0b6-e908-4111-8eb1-94c>

Federated Id

userPrincipalName

This way, ADFS will require PINPAD or Turing image in order to validate and access Office365, in addition to ADFS primary authentication policy.

# MI LABS ES Login

Welcome ES\office.user

For security reasons, we require additional information  
to verify your account

OTC:

1	2	3	4	5	6	7	8	9	0
8	5	1	0	9	8	7	2	0	4

[refresh](#)

[Continue](#)

## 16 Related Articles

- ADFS configuration

[https://kb.swivelsecure.com/w/index.php/Microsoft\\_ADFS\\_3\\_Authentication](https://kb.swivelsecure.com/w/index.php/Microsoft_ADFS_3_Authentication)

## **17 Additional Information**

For assistance in the Swivel Secure installation and configuration please firstly contact your reseller and then email Swivel Secure support at supportdesk@swivelsecure.com